Subcommittee on Government Operations
Hearing on
"FITARA 14.0"

July 28, 2022

Questions for the Record

Chairman Connolly

1. The Environmental Protection Agency (EPA) was one of three agencies to make progress toward establishing an information technology (IT) working capital fund since the last FITARA Scorecard. Why is the EPA establishing a working capital fund, and what are your plans for how it will help modernize IT?

Response: Under the authority of Section 403 of the Government Management Reform Act of 1994 and EPA's Fiscal Year 1997 Appropriations Act, EPA began operating its Working Capital Fund (WCF) on October 1, 1996. EPA does not use or desire the additional authorities for a WCF granted through the Modernizing Government Technology (MGT) Act. EPA's existing WCF provides a critical tool to collect and manage resources to fund IT hardware and services. The WCF is especially well-positioned to help EPA modernize our IT systems because it offers the ability to create multi-year services that allow the agency to strategically fund and support long-term enterprise IT needs without subjecting that funding to the uncertainty of the congressional appropriation process and long-term continuing resolutions.

2. Has the EPA developed a multi-cloud strategy?

Response: Yes. EPA has established multiple enterprise cloud platforms targeting a variety of use cases for application platforms and services, including Amazon Web Services, Microsoft Azure, SalesForce, and Cloud.gov. EPA's cloud strategy and guidance promote no-code and low-code as its preferred approaches for application architecture to encourage application migration and modernization efforts in order to leverage Software as a Service and Platform as a Service cloud targets.

3. What types of tools or processes do you use to assess risk across your IT/cloud environment?

Response: The EPA leverages annual independent third-party assessments as a part of its system security authorization processes as well as continuous monitoring reviews to assess risk across its IT/cloud environments. Specifically, EPA leverages an enterprise suite of Continuous Diagnostic and Mitigation tools that natively coordinates detection, prevention, investigation of security risks, vulnerabilities, and response across endpoints, identities, emails, and applications to provide integrated protection against sophisticated attacks. EPA also leverages cloud-native security risk management solutions to assess and manage risks associated with its cloud service providers. EPA has also implemented an Enterprise Risk Management process that employs an

overarching evaluation of EPA risks to determine if those risks are candidates for risk mitigation and acceptance or if corrective plans to remediate the vulnerabilities are required.

4. Do you rely on third party tools, National Institute of Standards and Technology (NIST) cybersecurity frameworks, or other?

Response: Yes. In addition to the capabilities referenced above, EPA employs the NIST Cybersecurity Framework, the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation program, and other commercial tools integral to EPA's risk management program. Additionally, EPA leverages frequent DHS cyber hygiene security scans and vulnerability disclosure services to assess risk across its IT environment.

5. Would the addition of dynamic scoring to FITARA help agencies better address the current threat environment?

Response: Cybersecurity risks and vulnerabilities are dynamic in nature, and information technology is constantly evolving to enable missions in a secure manner. Static scoring methodologies neither consider these dynamic changes, evolution, nor do they consider the resource adjustments needed to maintain a secure posture and address federal priorities. A dynamic scoring methodology that anticipates ongoing and new threats, as well as agency-planned strategies to achieve federal cybersecurity priorities and maintain an acceptable risk management posture, may be helpful in addressing the current threat environment.

6. What other tools would provide agencies better insight into the variability of an agency's cyber posture?

Response: Most recently, Federal Information System Modernization Act (FISMA) reporting has added the requirements to assess the ground truth testing of systems to detect vulnerabilities in the environment through red team exercises, penetration testing, and vulnerability disclosure platforms. While EPA currently leverages independent security assessments, DHS Cybersecurity Hygiene Scans, and the Vulnerability Disclosure Program platform; in the future, EPA will assess a capability or service to perform large-scale penetration testing across our Enterprise operating environment.

<u>Ranking Member Hice</u>

1. Your written testimony states that, "The forward focus for EPA will be a Cloud Smart rationalization of applications to drive application consolidation and cloud adoption."

a. How does EPA plan to track application consolidation and cloud adoption?

Response: Through the ongoing Agency IT Portfolio Review process, EPA will track application consolidation and cloud adoption across all Regions and Programs. The EPA Office of Information Technology Operations leads Cloud adoption.

b. Will the manner in which EPA tracks these activities generate a data set that Congress can use to measure EPA's success?

Response: EPA's approach establishes program and application-specific goals that are tracked and managed within the annual IT Portfolio Review Process. The application rationalization process is highly variable across applications and component organizations and does not support the generation of a tracking dataset. The path forward for each application must consider differing variables (e.g., funding, regulatory authority, program maturity, and burden on the regulated community and implementing states or tribes).

2. Your written testimony identifies cybersecurity as one of EPA's "top priorities." Yet in the FITARA 14.0, 13.0, and 12.0 Scorecards, EPA received "D" grades in the Cyber/FISMA category. Understanding that the FITARA 14.0 Scorecard had some data challenges for the Cyber/FISMA metric, please explain why a top priority would score so low on the prior two FITARA Scorecards.

Response: Cybersecurity and implementing President Biden's *Executive Order on Improving the Nation's Cybersecurity* remains a top priority for EPA, as evidenced in EPA's implementation of security metrics that resulted in an overall FISMA rating of "Managing Risk" and an OIG FISMA rating of "Effective, Level 3" for the last several years. Additionally, EPA has applied concerted efforts to maintain steady progress on FISMA metrics and *Executive Order on Enhancing the Nation's Cybersecurity* priorities.

Prior to scorecard 14.0 , the FITARA scorecard leveraged the OIG's FISMA assessment rating and the Agency's progress in achieving the prior Administration's Cross-Agency Priority (CAP) cybersecurity goals, which provided a more balanced rating. The FITARA 14.0 scoring methodology changed to only rely on the OIG assessment, whereby an "Effective, Level 3" rating equates to a "D" on the FITARA scorecard.

Under the FITARA 12.0 scorecard reporting timeframe, the EPA experienced a decrease in the Intrusion Detection and Prevention CAP goal sub-metric due to a second-level domain configuration error. While this initially resulted in a "D" grade, the error was corrected and verified via Department of Homeland Security scans.

The EPA continues to focus its efforts on improving its cybersecurity posture and has made considerable progress towards achieving its target metrics for Multifactor Authentication, Data Encryption, Logging Maturity, and Zero Trust Architecture. EPA's long-term performance goal, with respect to EPA's current strategic plan, is dedicated to tracking and communicating to Congress through the annual budget process EPA's progress in meeting these requirements of the EO.

3. Your written testimony emphasizes the importance of a strong cyber workforce because you state that, "EPA maintains a robust Cyber Workforce Plan with dozens of actions across multiple fiscal years to ensure a highly skilled and agile IT and cyber workforce." How might a future Scorecard track EPA's cyber workforce efforts and what metrics could it use to spotlight EPA's successes?

Response: A future Scorecard could track EPA's progress in meeting the milestones identified in its cyber workforce plan. EPA's plan has benefited the agency because it has tracked progress on meeting milestones related to hiring, retention, training, development, and building our future cyber workforce talent pipeline.

4. The description accompanying the Scorecard category titled "Enhanced Transparency and Improved Risk Management" says, "FITARA requires OMB to publicize detailed information on federal IT investments and requires agency CIOs to categorize their major IT investments by risk." EPA scored 70 percent on this category.

a. Please explain how EPA defines "risk" and a "major IT investment."

Response: The EPA's definition of "risk" is derived from OMB Circular A-11 and IT Budget Capital Planning Guidance. OMB Circular A-11 indicates, page 18 states: "Risk is the effect of uncertainty on objectives. Risk management is coordinated activity to direct and control challenges or threats to achieving an organization's goals and objectives." Per pg. 19 of the FY 22 IT Budget Capital Planning Guidance, "The Agency CIO rates each investment based on best judgment, using a set of pre-established criteria. As a rule, the Evaluation should reflect the CIO's assessment of the risk and the Investment's ability to accomplish its goals. CIOs should consult with appropriate stakeholders in making their evaluation, such as CAOs, program managers, etc. Evaluation ratings are scored on a five-point risk scale, as follows:"

CIO Risk Evaluation	**Color**
5 – Low Risk	Green
4 – Moderately Low Risk	Green
3 – Medium Risk	Yellow
2 – Moderately High Risk	Red
1 – High Risk	Red

To evaluate risk level for its major IT investments, the EPA uses an internal investment rating tool, which assesses certain investment rating factors, including Performance Management (includes Cost Variance, Schedule Variance, Performance Measures), Risk and Issue Management (includes Risks, POA&Ms, Corrective Actions), and Workforce Management (includes Contractor Oversight and Human Capital). Major IT investment personnel are asked to submit their assessment of their investments while the Capital Planning and Investment Control Team provides an independent assessment of the investment(s). Both assessments and recommendations are provided to the CIO, who makes the final decision regarding risk rating. In addition, the EPA recently worked with GSA/Folio Support to add a custom field in the Folio system to address compliance for Section 508, Multi-Factor Authentication, and encryption requirements. This was added during August 2022 and will be tracked going forward.

The EPA defines "major IT investment" as an IT investment that meets at least one of the criteria listed below:

- Is designated by the CIO as critical to the EPA mission or to the administration of programs, finances, property, or other resources,

- Is for financial management and obligates more than $500K annually,
- Requires special management attention because of its importance to the mission of EPA,
- Has a significant program or policy implication or Congressional interest,
- Has high executive visibility; and,
- Has high development, operating, or maintenance annual expenditure costs equal to or greater than $5M.

b. Does EPA's grade mean that 70 percent of its major IT investments are at risk? Please explain the significance of EPA's grade in this category.

Response: No. The EPA's grade in this category does not mean 70% of its major IT investments are at risk. During FY 22, all major IT investments are rated either Medium Risk (3/Yellow) or Moderately Low Risk (4/Green) (see 4a above).

c. What percentage of EPA's entire IT investment portfolio is comprised of "major IT investments?"

Response: During FY 22, the EPA's IT investment portfolio is comprised of 9.8% OMB Type 01 major IT investments (13 of 132 investments). Beginning in FY 23, the EPA's IT investment portfolio will be comprised of 9.1% OMB Type 01 major IT investments (12 of 132 investments).

5. During the hearing, Rep. Andrew Clyde asked you to provide an estimate of the resources required of the agency to put together the data feeding into this Scorecard. In providing the Committee with that response, please provide as much information as possible relative to the time, money, and staff it takes to collect and assemble the data for EPA's data submissions for the Scorecard.

Response: The EPA provides updates to the Federal IT Dashboard (ITDB) for 12 Major IT investments on a monthly basis and semi-annually for all of our 132 IT investments. The EPA conducts annual IT Portfolio Reviews (ITPRs) for 23 separate EPA Program and Regional offices. Additionally, the Integrated Data Collection (IDC) is collected and posted onto OMB MAX sites by various data owners on a quarterly basis. Staff members routinely coordinate the Capital Planning and Investment Control (CPIC) submissions via the Folio reporting system which feeds into the ITDB. The staff is augmented by contract support that requires approximately $502K/year (~10K hours/year) to perform and facilitate these reporting and ITPR efforts. Throughout the monthly and semi-annual CPIC submissions the staff facilitates data calls, assesses investments, provides communications and trainings on reporting system changes, manages issue resolution, and prepares and briefs leadership on investment status and assessments.

6. Are there categories not included in the Scorecard that could or should be added to better measure EPA's information technology and cybersecurity posture?

Response: For the cybersecurity category, the FITARA 14.0 scorecard is limited to OIG metrics that do not directly align with the *Executive Order on Improving the Nation's Cybersecurity* and subsequent OMB or CISA memorandum and directives on cybersecurity priorities. The FITARA scorecard do not reflect an actual change or downward trend in EPA's cybersecurity posture; rather reflects a change in the grading methodology. Providing metrics that align with the priorities federal agencies are working on (e.g., Cloud adoption, Identity and Access Management, etc.) would better measure IT and cybersecurity performance. The Agency continues to progress with FISMA metrics, EO 14028 compliance, deployment of CDM security capabilities, and hardening the information environment. Examples include 100% Assets covered by an ATO, increased adoption of multifactor authentication and data encryption, 98% of systems assets coved by smart patching, 100% implementation of the Vulnerability Disclosure Program, increased implementation of privilege access user management and deployment of an agency endpoint detection and response capability.